IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
Applicant: Julian Mitchell
Art Group: 2144
Serial No.: 10/037,043
Examiner: Bengzon
Filing Date: November 9th, 2001
For: "Middlebox Control"

AFFIDAVIT OF JULIAN MITCHELL

Maidenhead, Berkshire, United Kingdom

The undersigned, being duly deposed, swears and states that:

My name is **Julian Mitchell**, I live at 33 Suffolk Road, Maidenhead, Berkshire, SL6 2TG, United Kingdom. I was born in Sunderland, Tyne & Wear, United Kingdom and attended schools in Sunderland, Tyne & Wear, United Kingdom. I studied Electronic, Computer and Communications Engineering at the University of Bradford, West Yorkshire, United Kingdom. I hold a Batchelor of Engineering degree from The University of Bradford.

I am employed by Nortel Networks Limited ("Nortel"), assignee of United States Patent Application Serial Number 10/037,043 ("the Application"), as a member of its Scientific Staff and as an Individual Contributor working on telecommunications equipment software design. I am a specialist in Voice over Internet Protocol 'VoIP' policy architecture with particular emphasis on access policy, especially as it relates to border control, Network Address Translator 'NAT' traversal, and admissions control. I also represent Nortel at 3GPP standards meetings and am author of Internet Engineering Taskforce 'IETF' paper (draft) - 'draft-ietf-megaco-naspkg', 2000-2002 http://ietfreport.isoc.org/cgi-bin/id2pdf?f1=draft-ietf-megaco-naspkg-04.txt.

I am named as an inventor in respect of the Application, but I make this declaration in my capacity as an expert in the field of telecommunications and particularly in the field of VoIP access policy including border control, NAT traversal and admissions control.

I have considered the statements made by the Examiner in the Office Action mailed August 9, 2006 as they relate to the presently pending claims of the Application. I am familiar with the content of the Application and am also familiar with the disclosures of prior art references Schuster et al (US6822957), Huitema (IETF Working Document 'MIDCOM Scenarios'), Handley et al (IETF Working Document, RFC2327, 'SDP:Session Description Protocol'), Srisuresh et al (IETF Working Document 'Middlebox Communication Architecture and Framework'), Mahler et al (US6381638), Collins (US2003/0055978) and Xu et al (US2003/0114322).

At a high level, the invention as defined by current claim 1 of the Application builds on the known concept of communicating via middleboxes such as Network Address Translators 'NATs'. The invention provides a means of determining which is the appropriate one of a plurality of middleboxes in a communication network that a middlebox control node should communicate with to effect a communication with an

entity located within an address realm of said appropriate one of the plurality of middleboxes. Previously, it has been necessary for the middlebox control node to store information identifying which entities are located within the address realms of respective middleboxes to make this determination. The present invention provides a middlebox identity providing node that is separate from the middlebox control node that makes the determination of the appropriate one of the plurality of middleboxes on behalf of the middlebox control node, thereby relieving it from the burden of storing the aforesaid information. It is an essential feature of the arrangement that the middlebox control node is not located within the same address realm as that of any of the entities located within the address realms of the middleboxes, i.e. the middlebox control node is on an 'external' side of the address realms of the middleboxes relative to the entities connected to said middleboxes within respective address realms of said middleboxes.

Considering Schuster, in my opinion, none of devices 26, 38, 40 and 44 of figure 1 of Schuster can be considered as a NAT (middlebox) identity providing node since none of these devices functions to determine the identity of a NAT and to provide this to a NAT control node. The telephony proxy server 24 of Schuster is not a NAT control node. Even if it were considered so, none of the devices 14 through to 22 and 26 of computer network 12 operates to provide an identity of the router 26 to the telephony proxy server 24 because the telephony proxy server 24 already knows that all of the devices 14 through to 22 and itself are connected to each other within the address realm controlled by router 26 so no useful purpose would be served by any of devices 14 through to 22 and 26 sending the identity of router 26 to the telephony proxy server 24. Furthermore, there is nothing in the disclosure of Schuster that describes the telephony proxy server as sending messages to the router 26 to control it per se, i.e. the telephony proxy server 24 does not send NAT (middlebox) control messages as required by claim 1. Also, the telephony proxy server 24 is in the same address realm as the router or NAT 26 which is contrary to an essential limitation of the invention. Item 44 is not in fact a device at all but is a link layer of a layered protocol stack 42 of any of network devices 14 through to 24. Devices 38 and 40 comprise network switches. These switch devices 38 and 40 do not operate to determine the identity of router 26 or the identity of any other NAT and to provide this to any other device in the network. In my opinion Schuster does not teach any device which is operable to determine the identity of an appropriate one of a plurality of NATs based on information about an entity in a control message and to provide the identity of said appropriate one of the NATs to a NAT control node.

Claim1 of the Application creates five particular requirements for the method of the invention. These are that:

i) the (determined) middlebox must be in the same address realm as the entity whose address information is contained in the control message received by the middlebox identity providing node;

ii) the middlebox control node must be in a different address realm to that of the entity whose address information is contained in the control message received by the middlebox identity providing node;

iii) the middlebox identity providing node must be separate from the middlebox control node;

iv) the identity of the middlebox connected to said entity whose address information is contained in the control message received by the middlebox identity providing node must be sent to the middlebox control node; and

v) the middlebox identity providing node must be located in a control signal path from said entity to the middlebox control node.

None of devices 26, 38, 40 and 44 can satisfy all of the five foregoing conditions.

Item 44 is not in fact a device at all but is a link layer of a layered protocol stack 42 of any of network devices 14 through to 24. The link layer 44 includes a Network Interface Card 'NIC' for connecting the network devices 14 to 24 to computer network 12. As such, all of devices 14 to 24 are in the same address realm with router 26. It is the devices 14 to 24 that may themselves be supposed to be the middlebox identity providing node if the Examiner's argument with respect to item 44 is to be followed.

Taking device 24 of said devices 14 through to 24, the telephony proxy server 24 cannot satisfy condition iii) above because the middlebox identity providing node must be separate from the middlebox control node.

Taking devices 14 through to 22 of devices 14 to 24, none of devices 14 to 22 can satisfy conditions ii) or iv) and it is debatable whether any of these devices can satisfy condition v). For example, condition ii) requires the middlebox control node to be in a different address realm to that of the entity. Schuster describes only one NAT, namely router 26. Therefore, the one of the entities must be one of devices 14 through to 24. Since all of devices 14 to 24 are in the same address realm, condition ii) cannot be satisfied where the telephony proxy server 24 is the NAT control node. As already discussed above, condition iv) requires that the middlebox identity providing node sends the determined identity of the middlebox to the middlebox control node. None of devices 14 to 22 perform this operation and so condition iv) cannot be satisfied. Condition v) requires that the middlebox identity providing node is located in a signal path from said one of the entities to the middlebox control node. It is not apparent how the disclosure of Schuster can satisfy this condition in respect of devices 14 to 24.

Considering router 26 as the identity providing node. None of conditions ii), iv) or v) can be satisfied. Router 26 is clearly in the same address realm as telephony proxy server 24 so condition ii) cannot be satisfied. No purpose would be served by router 26 providing itself with its own identity so condition iv) cannot be satisfied. Rouer 26 is not in the control signal path from any of devices 14 to 22 (said one of the entities) to the telephony proxy server 24 (control node) so condition v) cannot be satisfied.

Switches 38 and 40 are not middlebox identity providing nodes since they do not operate to determine the identity of a middlebox based on information concerning an entity in a control message. That being said, switches 38 and 40 cannot satisfy conditions i), ii) iv) or v). Condition i) cannot be satisfied because any messages received by switches 38 and 40 do not identify the entity in computer network 12 controlled by router 26. The router 26 functions as a NAT to effectively hide the identity of any of devices 14 to 22 from switches 38 and 40 providing them instead with the public address of computer network 12. Condition ii) cannot be satisfied for the reasons already explained above. Condition iv) cannot be satisfied because switches 38

and 40 do not operate to determine the identity of router 26 and send this to telephony proxy server 24. Condition v) cannot be satisfied because switches 38 and 40 are not in the control signal path from said one of the entities (14 to 22) to the middlebox control node (server 24).

Even if the Examiner were to rearrange which devices of Schuster he considers as constituting the said one of the entities, the middlebox, the middlebox control node or the middlebox identity providing node, there is no arrangement of devices in Schuster that can satisfy all of the above conditions.

The Examiner has identified column 19, lines 15 to 30 of Schuster as describing the feature of 'receiving a control message at a NAT identity providing node in the communications network, said control message comprising information about one of the entities in the communications network'. However, what this part of Schuster makes no mention of receiving a control message at a NAT identity providing node as there is no mention of providing the identity of the NAT. In fact, what this part of Schuster describes is how a control message may be modified to allow it to work through a NAT which is not the same thing at all.

I note that the only contribution considered as being offered by Huitema is that it discloses that a NAT may be a middlebox. Therefore, based on my analysis of Schuster and Huitema, there can be no combination or construction of these documents that teaches or suggests all of the features of claim 1 of the Application as currently under consideration.

Similar considerations apply to independent claims 18, 23, 24, 25 and 27.

Considering claims 2 and 3, figures 13 and 14 of Schuster show procedures within a NAT but do not show the adding to a control message of any NAT identity. Column 23, lines 20 to 25 describe well known ports and has nothing to do with adding NAT identity information to a call set up message or adding additional information.

Considering claim 6, column 19, lines 15 to 30 of Schuster do not describe adding a NAT identity to a call set up message.

Similar observations can be made in respect of other sections of Schuster referred to in the Office Action.

Considering Xu, in my opinion none of devices 14(a), 14(b) or 20 comprises a NAT/firewall identity providing node since none of these devices operates to identify from entity information in a control message any of NAT/firewalls 32(a) or 32(b) and to provide said identity to the CCM server 18 (middlebox control node).

It is clear from paragraphs 0041 through to 0047 and paragraph 0061 that each of the NAT/firewalls 32(a) and 32(b) operates in a conventional manner to translate between private network IP address/port pairs for devices (30(a) to (f)) within their respective address realms and public IP address/port pairs. The NAT/firewalls themselves provide their own identities in a conventional manner to other devices within the network through the translation mechanism. In particular, the NAT/firewalls 32(a) and 32(b) provide their own identities to CCM server 18 (middlebox control node) through the

translation mechanism whereby when 'a first media datagram, addressed to the CCM RTP channel, being originated by the first client 30(a) and received by the CCM server 18. Because the first client 30 is coupled to the Internet 12 through the NAT server 32(a), the NAT server 32(a) translates the source IP address of the datagram from the private network IP address of the first client 30(a) to the public IP address of the NAT server 32(a) and translates the port number from the port number assigned by the first client 30(a) to a port number assigned by the NAT server 32(a)', paragraph 0061 (emphasis added). Thus, the CCM server receives the identity of the NAT/firewall 32(a) from the address translated datagram and thus directly from the NAT/firewall.

Paragraph 0049 of Xu describes 'When initiating a media session the first client, client 30(a) for example, may provide the proxy server with which the first client 30(a) is registered, proxy server 14(a) for example, with identity of the second client to which it would like initiate a media session, client 30(d) for example. The proxy server 14(a) then interrogates the directory server 20 to determine with which proxy server the second client 30(d) is registered, proxy server 14(b) for example. The two proxy servers 14(a) and 14(b) then facilitate the exchange of messages for setting up the media session, for communicating other messages representing media session negotiation between each of the first client 30(a) and the second client 30(d), and for directing each of the first client 30(a) and the second client 30(d) to route media datagrams to the CCM server 18 during the media session'. The function of each of the proxy servers 14(a) and 14(b) therefore is to interrogate the directory server 20 to determine with which proxy server another client device is registered. The function of the directory server 20 is to provide the identity of the proxy server with which said another client device is registered. None of the proxy servers 14(a) and 14(b) or the directory server 20 operates to identify either of the NAT/firewalls 32(a) or 32(b) and to provide this identify to the CCM server 18.

Thus, what Xu describes is quite different in a number of respects to the invention as described in claim 1. In fact, it is clear that, since the NAT/firewalls 32(a) and 32(b) operate to perform address translation in a conventional manner, there is no requirement to send control messages from a middlebox control node as required by claim 1.

Furthermore, if any of the devices in the system described in Xu did operate as contended to identity a middlebox associated with an entity and to provide the middlebox's identity to a middlebox control node such that the middlebox control node could send middlebox control messages to said middlebox, the problem identified in paragraph 0056 of Xu would not arise, whereby 'because the second client 30(d) is on the private network 34(b) and can only communicate with the proxy server 14(b) through the NAT server 32(b), the proxy server 14(b) may not be able to initiate the sending of the media session signaling message to the second client 30(d) but instead may have to wait for the second client 30(b) to poll the proxy server 14(b) for the media session signaling message or to update its registration with the proxy server 14(b) such that the proxy server 14(b) can initiate the media session signaling message as a reply frame to the registration update frame such that the media session signaling message will be routed to the second client 30(d) through the NAT server'. The existence of the foregoing problem confirms that the system of Xu does not operate in the manner suggested since, if it did so, the problem would not occur.

Paragraph 0051 of Xu does not disclose using the NAT/firewall identity providing node to determine the identity of a NAT/firewall connected to said one entity in its respective one of the plurality of address realms. What paragraph 0051 states is that 'Step 36 represents the first client 30(a) sending a media session signaling message to the proxy server 14(a) to which the first client 30(a) is registered. The media session signaling message may be a SIP compliant "Invite" message and may identify: 1) the second client 30(d) as the client with which the first client 30(a) would like to initiate a media session, and 2) a first client network address established by the first client 30(a) for receipt of media datagrams during the media session. The first client network address may include the IP address of the first client 30(a), which is a private network address, and a first client port number assigned to the media session by the first client 30(a)'. Since the address received by the proxy server 14(a) comprise a private network address of the first client 30(a), it is unclear how the proxy server 14(a) uses this to determine the identity of NAT/firewall 32(a) or 32(b). In fact, it does not since no useful purpose would be served by its doing so. Furthermore, nowhere in Xu is it described that any of the proxy servers 14(a) or 14(b) or the directory server 20 sends the identity of the NAT/firewall 32(a) or 32(b), determined by it, to the CCM server 18. As already indicated, the NAT/firewall 32(a) or 32(b) provides its own identity to the CCM server 18 through the address translation mechanism.

I note that the only contribution considered as being offered by Huitema is that it discloses that a NAT may be a middlebox. Therefore, based on my analysis of Xu and Huitema, there can be no combination or construction of these documents that teaches or suggests all of the features of claim 1 of the Application as currently under consideration.

Similar considerations apply to independent claims 18, 23, 24, 25 and 27.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the Application or any patent issued thereon.

Signed by

JE Mitchell

Julian Mitchell

At Maidenhead this 4th day of December, 2006